Voicemail Hacking

Quick, what's your voicemail PIN? Don't know? It could be a default PIN, such as 1-2-3-4-5. Or maybe it was never set up at all. Facing a myriad of online and device threats, security experts warn that voicemail system security is often overlooked on both personal and business accounts..

Voicemail system vulnerability

If you don't change the default password on all your voicemail accounts, you – or your company – could be in for an expensive surprise. There are hackers who know how to compromise voicemail systems to steal personal and financial information, or to gain access to your financial and social media accounts by intercepting two factor account verification codes. Some hackers have reportedly monitored incoming voicemail messages at businesses and responded to callers by text, impersonating the business, These texts include links for payments on requested services, which go to the hackers' accounts.

Hackers have been known to hijack voicemail accounts and change outgoing messages so they will accept automated international collect calls, which get added to the mailbox owners phone bill. In another version of this scam, a hacker breaks into a voicemail system's call forwarding feature, programs the system to forward calls to an international number, then uses it to make calls.

In the past, hackers typically targeted business voicemail systems, but consumers with residential voicemail should also beware.

You should know

- Hackers may try to break into business voicemail systems during holiday periods or weekends, when changes to outgoing messages are less likely to be noticed.
- Hackers are often based internationally, with calls originating in, and routing through, many countries around the world.
- In international collect call scams, business victims may not find out they've been hacked until their phone company reports unusual activity; and residential victims may not find out until they receive unusually high phone bills.

Tips to minimize your risk

To avoid falling prey to this scam, follow these helpful tips:

- Always change default passwords for all voicemail boxes, at work, at home and on your mobile phone.
- Choose a complex voicemail password of at least six digits.
- Change your voicemail password frequently.
- Don't use obvious passwords such as an address, birth date, phone number, repeating numbers, such as 000000, or successive numbers, such as 123456.
- Check your recorded announcement regularly to ensure the greeting is indeed yours.
- Consider blocking international calls.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau

- Disable remote notification, auto-attendant, call-forwarding and out-paging features if you don't use them.
- Consult your voicemail service provider about additional security precautions.

If you think you've been hacked, report the incident to both your service provider and the police.

Filing a complaint

You have multiple options for filing a complaint with the FCC:

- File a complaint online at https://consumercomplaints.fcc.gov
- By phone: 1-888-CALL-FCC (1-888-225-5322); ASL: 1-844-432-2275
- By mail (please include your name, address, contact information and as much detail about your complaint as possible):

  Federal Communications Commission
  Consumer and Governmental Affairs Bureau
  Consumer Inquiries and Complaints Division
  45 L Street NE
  Washington, DC 20554

Alternate formats

To request this article in an alternate format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed 10/06/22